Department of Homeland Security Daily Open Source Infrastructure Report for 7 August 2008

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

- According to CNN, 11 people were indicted Tuesday for allegedly stealing more than 40 million credit and debit card numbers. It is believed to be the largest hacking case that the U.S. Justice Department has ever tried to prosecute. (See item **13**)
- Fox News reports that a map of the U.S. president's motorcade route to Camp David was found last week when police searched the Bethesda, Maryland, home of a teenager accused of stockpiling weapons and bomb-making materials. (See item **27**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *August 4, Arab Times* – (International; National) **'Iran could easily shut Hormuz.'** Iran can easily close a key Gulf shipping route if it were attacked over its nuclear program, the head of the Revolutionary Guards was quoted as saying on Monday, a move that could choke off world oil exports. Iran's armed forces have "the possibility of closing the Strait of Hormuz, easily and on an unlimited basis," state radio quoted the Iranian official. As well as threatening to shut the Strait of Hormuz, he said the elite Guards force had tested a naval weapon that could destroy any vessel in a range of 190 miles, media said. Iran's recent missile tests rattled oil markets. About 40 percent of world oil exports passes through the Strait of Hormuz, a choke point at the southern end of the

Gulf, flanked by the coastlines of Iran and Oman. Much of it goes to Asia, the U.S., and western Europe. The U.S. military has pledged to keep the Strait open.
Source: http://www.arabtimesonline.com/client/pagesdetails.asp?nid=20530&ccid=11

2. *August 6, Reuters* – (Illinois; Indiana) **Power back for most customers in Illinois and Indiana.** Power companies in Illinois and Indiana restored electricity to most customers affected by severe thunderstorms Monday night, but still had about 100,000 customers without service, local power companies said Wednesday morning. The storms affected service to more than 637,000 homes and businesses in Illinois and Indiana. Exelon Corp.'s Commonwealth Edison (ComEd) unit reported about 56,000 customers still in the dark Wednesday morning. ComEd, which serves customers in Chicago and northern Illinois, expects to restore service to all customers by Friday night. In Indiana, NiSource Inc.'s Northern Indiana Public Service Co. (NIPSCO) unit reported about 27,000 customers still without power Wednesday morning. NIPSCO said it expected to restore power to all customers by late Thursday. In central and southern Illinois, Ameren Corp. reported 11,000 customers without power.
Source:
http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN0641662520080806

[Return to top]

Chemical Industry Sector

3. *August 6, iStockAnalyst*– (Oregon) **Oregon issues first report on state chemical use.** More than 40 million pounds of pesticides and herbicides were used in Oregon's farms, forests and fields last year, with potato fields getting the biggest dose, according to the state's first tabulation of chemical use. The state Department of Agriculture report showed that a soil fumigant used on potato fields, known as metam-sodium, was by far the most-applied product by weight. It accounted for 42 percent of the chemicals applied last year. The report was authorized by the 1999 Legislature to provide more detailed information about the use of toxic chemicals in agriculture, to gauge how they affect soil and water quality. It was released last week after being delayed by years of political struggle. During the political fight to establish the reporting system, the agriculture industry opposed detailed public disclosure of chemical use in smaller geographic areas, saying that information could be misused. Rounding out the top five statewide after metam-sodium were the herbicide glyphosate at 9 percent of the total weight, the wood preservative copper naphthenate at 7 percent, the soil fumigant 1,3-dichloropropene at 5 percent and the insecticide aliphatic petroleum hydrocarbons at 4 percent. Agriculture accounted for nearly all of the chemical use, with almost 85 percent of the total. That was followed by other at 9 percent and forestry at 3 percent. According to the report, the state received almost 285,000 reports of herbicide and pesticide use. A total of 551 different chemicals were cited.
Source:
http://www.istockanalyst.com/article/viewiStockNews+articleid_2481427~title_Oregon-issues-first.html

4. *August 6, Associated Press* – (Iowa) **Chemical leak at ice rink leads to mall evacuation.** Emergency officials say part of Coral Ridge Mall in Coralville, Iowa, had to be evacuated after a chemical leak at an ice rink. Emergency crews were called to the mall around 7 p.m. on Tuesday because of the leak in a mechanical room at the ice rink. The chemical was a refrigerant used to freeze the ice. An Assistant Fire Chief says the theaters, ice arena, mall food court and all stores between the ice arena and Target were closed and evacuated. No one was injured, though several people reported feeling some effects, including headaches.
   Source: http://www.chicagotribune.com/news/chi-ap-ia-mallevacuated,0,3537964.story

5. *August 5, KPSP 2 Palm Springs* – (California) **Hazmat incident in La Quinta hospitalizes two.** Riverside County, California, firefighters along with HAZMAT are on the scene of an unknown substance leak at the Eisenhower Urgent Care Facility, Highway 111 at Washington Street in La Quinta. Two adults have been taken to an area hospital with respiratory discomfort. 24 firefighters responded to the call. Between 25-30 persons were in the urgent care at the time of the leak.
   Source: http://www.deserttelevision.com/Global/story.asp?S=8794642

6. *August 3, Scranton Times Tribune* – (National) **Chemical storage data restricted after 9/11.** The lack of public awareness regarding storage of dangerous chemicals is getting even worse, critics say, as the government reduces reporting requirements and restricts access to information. The disclosure reports that chemical-storing companies must file with the Environmental Protection Agency (EPA) are inaccessible and about to become less informative. Risk-management plans were intended to be easily accessible to the public, but after 9/11, facility owners submitting the plans and the EPA became wary of releasing the information, said a lead environmental engineer and team leader for the Chemical Accident Prevention Program for EPA's Mid-Atlantic Region. As a result, the EPA removed the plans from its Web site a few months after the terrorist attack and requires the public to travel to a regional EPA office to view the files in person, by appointment. In July 2005, after several years of resistance from the EPA, the courts granted OMB Watch the right to republish plans online. Complete risk-management plans for all reporting facilities in the U.S. are available on the Right to Know Network Web site, www.rtknet.org. The risk-management plans available on the Right to Know Web site will change, however, once amendments made by the EPA in 2004 come into effect. The amendments no longer require facility managers to include off-site consequences of spills or explosions in the reports. This means no one will know the scope of potential danger to the surrounding public.
   Source: http://www.scrantontimes.com/articles/2008/08/03/news/sc_times_trib.20080803.a.pg7.tt03chemicalsside_s1.1827912_top3.txt

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

7. *August 6, Chicago Tribune* – (National) **Higher nuke waste disposal cost seen.** Even if no new reactors are built, getting rid of the country's nuclear waste will cost $96.2

billion and require a major expansion of the planned Nevada waste dump beyond limits imposed by Congress, the U.S. Energy Department said Tuesday. The revised cost estimate is for the proposed Yucca Mountain nuclear waste dump, 90 miles northwest of Las Vegas. The figure is $38.7 billion more than was anticipated in 2001.
Source: http://www.chicagotribune.com/news/nationworld/chi-nat-nuclear-wasteaug06,0,6053859.story

8. *August 6, Reuters* – (Michigan) **Entergy shuts Mich. Palisades reactor for work.** Entergy Corp. shut the Palisades nuclear power station in Michigan for work on August 5, a spokesman for the plant said Wednesday. He said the unit was currently in hot shutdown Mode 4 and would be going to cold shutdown Mode 5. Electricity traders guessed that with the unit going to cold shutdown, the outage could last about a week. At the time of the shutdown, the spokesman said operators were reducing the unit from full power for a planned shutdown to work on a control rod drive mechanism due to excessive leakage discovered over the weekend. Operators immediately shut the unit from 96 percent power when "the site experienced excessive unidentified leakage" of about four gallons per minute for short periods, the company said in a report to the U.S. Nuclear Regulatory Commission.
Source: http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN0646320820080806?pageNumber=1&virtualBrandChannel=0

9. *August 6, U.S. Nuclear Regulatory Commission* – (Illinois) **Loss of 84 of 94 emergency sirens due to inclement weather.** On Monday, a severe thunderstorm moved through Ogle County, and 84 of 94 emergency sirens for Byron Station became inoperable. There is currently no estimated time of repair due to the severe number of power outages. Sirens affected provide coverage for Ogle County and a small portion of Winnebago County. These are utility owned sirens. These sirens are not shared with other sites. In the event of a need for the sirens, a contingency plan using a "route alert" by the state will be implemented. There are no off-site power or grid concerns. Troubleshooting and restoration activities continue for the emergency sirens. Thirty-three sirens remain inoperable.
Source: http://www.nrc.gov/reading-rm/doc-collections/event-status/event/2008/20080806en.html

10. *August 5, U.S. Nuclear Regulatory Commission* – (Minnesota) **NRC begins special inspection at Prairie Island nuclear plant due to reactor trip.** The U.S. Nuclear Regulatory Commission (NRC) is conducting a special inspection at the Prairie Island Nuclear Power Station to review the causes of a reactor trip (automatic shutdown) and a subsequent trip of one of two auxiliary feedwater pumps. On July 31, Prairie Island Unit 1 reactor tripped and was shut down safely. Unit 2 was not affected. NRC Region III dispatched a three-person special inspection team to the plant to review the root causes of the reactor trip and the turbine driven auxiliary feedwater pump issue. The special inspection will also review the utility's response to the situation and the company's corrective actions. The average duration of a special inspection is seven days. The inspection report will be issued about 45 days after the inspection is complete. When

Unit 1 was being returned to service on August 3, plant operators declared an unusual event due to elevated levels of hydrazine in the turbine building. The company terminated the unusual event later on the same day when levels of hydrazine were successfully reduced. The special inspection team will review the circumstances around the unusual event.
Source: http://www.nrc.gov/reading-rm/doc-collections/news/2008/08-030.iii.html

[Return to top]

Defense Industrial Base Sector

11. *August 6, Military & Aerospace Electronics* – (National) **Kongsberg to supply Protector Remote Weapon Stations to U.S. Air Force.** Kongsberg Defence & Aerospace AS won a $28.8 million contract from the U.S. Air Force and the U.S. Army for deliveries of the Protector Remote Weapon Station (RWS). Common Remotely Operated Weapon Station (CROWS II) is a joint acquisition program for weapon stations for the U.S. Army's vehicle programs. This common solution will result in substantial efficiency gains in respect to protection, training, support, and further development. The Protector RWS, in the CROWS II configuration, enhances troop protection and lethality by providing soldiers with the ability to acquire and engage targets while inside the safety of a vehicle. The Protector RWS is designed to mount on various vehicle platforms and support numerous weapon systems.
Source: http://mae.pennnet.com/Articles/Article_Display.cfm?Section=ONEWS&PUBLICATION_ID=32&ARTICLE_ID=336270&C=ONEWS&dcmp=rss

[Return to top]

Banking and Finance Sector

12. *August 6, Business Week* – (National) **Prosecutors take down alleged online scam.** On August 5, federal investigators raided the founder of the company Ad Surf Daily (ASD) office and the Bowdoin home in Quincy, Florida, and filed a civil complaint against the company. The U.S. Attorney's office in Washington, D.C., alleges in the suit that ASD defrauded more than 100,000 people with promises of online riches. Prosecutors, who seized more than $53 million in ASD assets from Bank of America (BAC), had been alerted to the alleged scam by numerous complaints, including many from children whose parents had been enticed by ASD's online promotional material. In the complaint, prosecutors contend that Ad Surf Daily, which operated out of a flower shop in Quincy, had no legitimate business model. Instead, the company relied on new investors to pay old investors—the definition of a Ponzi or "pyramid" scheme. ASD used online videos to become one of the most successful companies at drawing in participants. Government officials believe that ASD raked in more than $100 million with its seemingly sincere YouTube videos and podcasts, broadcasting the new business opportunities in the online advertising market. ASD members used that new Web technology over the weekend to calm clients who found their bank accounts frozen.

Source: http://www.businessweek.com/technology/content/aug2008/tc2008086_509247.htm?chan=top+news_top+news+index_news+%2B+analysis

13. *August 5, CNN* – (National) **Justice: Hackers steal 40 million credit card numbers.** Eleven people were indicted Tuesday for allegedly stealing more than 40 million credit and debit card numbers, federal authorities said. The indictments, which alleged that at least nine major U.S. retailers were hacked, were unsealed Tuesday in Boston, Massachusetts, and San Diego, California, prosecutors said. It is believed to be the largest hacking case that the Justice Department has ever tried to prosecute. Three of the defendants are from the United States; three are from Estonia; three are from Ukraine, two are from China and one is from Belarus. The remaining individual is known only by an alias and authorities do not know where that person is. Under the indictments, three Miami, Florida, men are accused of hacking into the wireless computer networks of retailers including TJX Companies, whose stores include Marshall's and T.J. Maxx, BJ's Wholesale Club, OfficeMax, Barnes and Noble and Sports Authority, among others. The three men installed "sniffer" programs designed to capture credit card numbers, passwords and account information as they moved through the retailers' card processing networks, said a U.S. attorney in Boston. The three then concealed the data in encrypted computer servers they controlled in the United States and Eastern Europe, the Justice Department said. Some credit and debit card numbers were sold on the Internet, and were "cashed out" by encoding the numbers on the magnetic strips of blank cards. "The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs," authorities said. They used anonymous Internet-based currencies to conceal and launder their proceeds, as well as channeling funds through bank accounts in Eastern Europe, the department said. "The 41 million credit and debit numbers were used internationally," said the attorney.
Source: http://www.cnn.com/2008/CRIME/08/05/card.fraud.charges/index.html

[Return to top]

Transportation Sector

14. *August 6, Reuters* – (Texas) **Houston, Sabine ship channels open with limits.** The Houston and Sabine Pass ship channels were open Wednesday but with restrictions on ship size after being shut Monday by Tropical Storm Edouard, the U.S. Coast Guard and ship pilots said. The limits will allow most ships to transit the Houston channel, according to the Coast Guard. Bulk crude carriers will be prevented from moving through the Sabine Pass channel, ship pilots said. At the Sabine Pass Channel, which serves refineries at Beaumont and Port Arthur, Texas, ships with a draft of 30 feet or less can enter or exit the waterway, according to the Sabine Pass ship pilots association. It could be Friday before the restrictions are lifted at the Sabine Pass channel, the ship pilots association said. At Houston, a survey by the U.S. Army Corps of Engineers must take place before the restrictions will be lifted.
Source: http://in.reuters.com/article/oilRpt/idINN0643210220080806

15. *August 5, Associated Press* – (California) **Jet evacuated after emergency landing at**

LAX. Passengers were evacuated by inflatable chutes Tuesday after an American Airlines Flight to Honolulu made an emergency landing at Los Angeles International Airport because someone smelled smoke in the cabin. No sign of fire was found on the aircraft. The plane was carrying 188 passengers and six crew members.
Source: http://ap.google.com/article/ALeqM5gdFehzqpv5i-WJ6iFr6DrB6C9UWwD92CENN00

16. *August 5, MSNBC* – (National) **Federal bridge database flawed.** Last week, msnbc.com uncovered Federal Highway Administration e-mails that show the feds' bridge inventory database is flawed. Msnbc.com says the newly released e-mails show: Kentucky was threatened with loss of federal funds for not turning in its bridge data; Iowa bridge engineers expressed frustration that they were not certified to inspect bridges, considering that they were considered qualified enough to design them; Mississippi lost federal aid funds in February for seven cities that failed to post or close unsafe bridges, a month after msnbc.com had reported on the reluctance of federal officials to withhold funds when states didn't meet inspection deadlines. Among the collections (mostly PDF files) that msnbc.com released were: A list of the steel deck truss bridges that were reinspected; A list of the bridges that had been misclassified as steel deck trusses; State-by-state summary of the reinspection results; State-by-state comparison of inspection programs 2006 (Excel file); "Issues of Concern" slide show by Tom Everett team leader of the bridge program at the Federal Highway Administration; and talking points for the administrator of the Federal Highway Administration.
Source: http://www.poynter.org/column.asp?id=2&aid=148022

17. *August 5, Occupational Health & Safety* – (National) **Senate approves Railroad Safety Enhancement Act.** The U.S. Senate has approved legislation designed to make America's railroads safer for train passengers and railroad employees, as well as people who drive across or live next to railroad tracks. The federal rail safety programs have not been reauthorized since 1994. The senator, who authored and introduced the measure last year, said the bill--the Railroad Safety Enhancement Act of 2007--addresses three industry-wide safety concerns: Employee fatigue under the "hours of service" laws; New safety technology, or "Positive Train Control" (PTC); and Grade crossing safety.
Source: http://www.ohsonline.com/articles/66098/

[Return to top]

Postal and Shipping Sector

18. *August 6, WISN 12 Milwaukee* – (Wisconsin) **Brookfield police investigate pipe bomb explosion.** A pipe bomb explosion inside a condominium complex could have killed someone, Brookfield, Wisconsin, police said. Police said someone put the pipe bomb inside the mailbox early one morning in July. When the bomb went off, it destroyed four other mailboxes. Shrapnel flew everywhere, and the mailbox door was found in the neighbor's back yard. Brookfield police said this was not typical vandalism. It was much more serious, and they are very concerned because someone could have really been hurt. The Bureau of Alcohol, Tobacco, and Firearms is assisting in the

investigation.
Source: http://www.wisn.com/news/17110080/detail.html

19. *August 5, WPTA 21 Fort Wayne* – (Indiana) **Ticking package.** The Fort Wayne Police Bomb Squad was called to Fire Station Ten August 5 after a Fed-Ex employee noticed a ticking sound in one of her packages and sought assistance. Firefighters immediately removed the package from the truck and called the bomb squad to find it was a room key encoder used in hotels. It took crews a little more than an hour to clear the scene.
Source: http://www.indianasnewscenter.com/news/local/26286679.html

[Return to top]

Agriculture and Food Sector

20. *August 6, Associated Press* – **Putting the squeeze on salmonella.** At a Virginia Tech laboratory this summer, food scientists subjected small grape tomatoes to what is called "high pressure processing" (HPP) to see if they could squeeze salmonella to death. In order to kill the bugs without affecting the food they are in, the key is to choose a water-packed food with few air pockets. Foods treated by HPP already are on the market, particularly raw oysters and processed meats. A different approach under consideration by the Food and Drug Administration (FDA) is irradiation, zapping fruits and vegetables with enough electron beams or other radiation to kill germs. While irradiated foods initially caused some consumer concern, government scientists make clear that the food itself harbors no radiation. The director of the Grocery Manufacturers Association's food laboratory trade association has petitioned the FDA to allow the irradiation levels for produce pathogen and other ready-to-eat foods, and hopes for approval by year's end.
Source: http://telegraphjournal.canadaeast.com/magazine/article/375774

21. *August 6, Associated Press; San Francisco Chronicle* – (National) **Investigation shows 'next time' is likely.** An investigation that should have taken hours or days instead has stretched on for weeks and months, the chairman of the House Energy and Commerce Committee said at hearings last month. One agency probably zeroed in on tomatoes too early, the committee concluded, while a second failed to tap industry and states' expertise in trying to trace the source of the contamination. Imports of fresh fruits and vegetables are soaring, and much of the produce comes from poorer countries where not all farms meet high sanitation standards. A typical American meal, said Tennessee's top epidemiologist includes foods from six countries. The Centers for Disease Control and Prevention estimates that 76 million Americans get sick every year from food contamination, 325,000 are hospitalized, and 5,000 die. A former associate Food and Drug Administration (FDA) commissioner testified that the agency can inspect the 120,000 U.S. food-processing facilities only once a decade, and the 200,000 foreign facilities exporting food to the United States "are almost never inspected by the FDA."
Source: http://www.chicagotribune.com/news/nationworld/chi-salmonella_charticleaug06,0,2634597.story

22. *August 6, San Jose Mercury News* – (International) **Lead found in two brands of**

imported candy. Health officials issued a warning Tuesday about two types of candy from Mexico and Malaysia that are laced with lead and could cause severe medical problems. The candies in question are Huevines confitados sabor chocolate imported from Mexico and Ego hao jin bang candy imported from Malaysia. Tests conducted by the California Department of Public Health found levels of lead that could cause health problems, and officials say consumers should throw away the candy.
Source:
http://www.mercurynews.com/localnewsheadlines/ci_10112715?nclick_check=1

23. *August 5, Associated Press* – (Wisconsin) **New invasive species discovered in Wisconsin.** Wisconsin officials have confirmed the first appearance of the emerald ash borer, a destructive pest believed to have begun its American spread in Michigan. The metallic-green insect is native to Asia and was first discovered in the Detroit area in 2002. It has killed an estimated 25 million trees across nine states. Wisconsin wildlife and agriculture officials say forest health specialists discovered the creature while investigating a report of ash trees dying near Newburg in southeastern Wisconsin. State officials say they will ban movement of firewood to fight the spread.
Source: http://www.mlive.com/newsflash/index.ssf?/base/news-56/121791174216830.xml&storylist=newsmichigan

[Return to top]

Water Sector

24. *August 6, Lower Hudson Journal News* – (New York) **Strontium 90 found in well near nuke plant.** In New York, trace amounts of radioactive strontium 90 have turned up in monitoring wells outside Indian Point's property for the second time in little more than a year. The concentrations in groundwater south of the plant, on the neighboring Lafarge factory property, are low enough that Entergy Nuclear officials say it is improbable that the contamination originated at the power plant. More likely, plant officials say, the strontium 90 remained in the atmosphere after nuclear weapons testing during the Cold War and made its way to underground water pathways. U.S. Nuclear Regulatory Commission (NRC) officials said Tuesday that they would speed up the testing of a split sample of water they took with Entergy workers from a monitoring well about 1,500 feet from Indian Point's property line. The level is so low that the experts are not sure whether it is more than simply background radiation, said an NRC spokesman. "But it does involve off-site groundwater," he added. NRC and county officials said there was no threat to public safety. The monitoring wells test for contamination in groundwater, not drinking water.
Source: http://www.lohud.com/apps/pbcs.dll/article?AID=2008808060357

25. *August 5, Union* – (California) **Arsenic and old mines: how to fix bad drinking water.** Some western Nevada County, California, households that have relied on under-the-sink filters to remove arsenic from their drinking water for the past decade could soon get relief, according to federal officials. A hearing is scheduled next week to address public concerns of drinking water contaminated by the abandoned Lava Cap Mine, a gold and silver mine that operated from 1961 and 1943. A week from today, Environmental

Protection Agency representatives will give background on the Superfund site and proposed alternatives to remedy the tainted groundwater found beneath it. Early water samples taken at the property showed eight to ten wells serving five households with arsenic levels above safe drinking water standards, said the remedial project manager for the site. Ingesting arsenic contaminated drinking water is known to cause cancer to humans. Absorption of arsenic through the skin by bathing or washing is considered a minimal health risk. Cleaning up the ground water is the second phase of the Superfund project. In recent years, construction crews worked to place a plastic and earthen cap over four acres of toxic mine tailings.
Source:
http://www.theunion.com/article/20080805/NEWS/679659426/1066/OPINION&parentprofile=-1

[Return to top]

Public Health and Healthcare Sector

26. *August 6, eFluxMedia* – (National) **FDA's new guidelines limit conflict of interest among advisers.** The Food and Drug Administration (FDA) on Monday issued final guidelines that seek to limit conflicts of interest among advisory committee members and open their procedures to public examination, the San Francisco Chronicle reported. Outside experts may not participate in federal advisory committee meetings on drugs and medical devices if they have a personal financial stake of more than $50,000 in a company affected by a matter under discussion, the agency said. Advisers with grants or other financial interests amounting to less than $50,000 may be allowed to attend meetings and vote if their expertise is deemed essential. The FDA may allow a specialist with a lesser financial interest to participate if there is "an essential need for the adviser's particular expertise," the agency said in a statement. Drug and device makers often pay lucrative consulting and speaking fees to the advisory committee members, who represent the world's leading authorities on a particular disease or condition. Under the guidelines released a year ago, experts with conflicts of up to $50,000 would have been permitted to attend committee meetings, but not to vote. The guidelines also allow FDA in certain cases to prohibit participation on advisory committees by some medical experts, regardless of whether they have more than a $50,000 financial interest.
Source:
http://www.efluxmedia.com/news_FDAs_New_Guidelines_Limit_Conflict_of_Interest_among_Advisers_21597.html

[Return to top]

Government Facilities Sector

27. *August 6, Fox News* – (Maryland) **Maryland teen allegedly had weapons, map of Camp David.** A map of the U.S. president's motorcade route to Camp David was found last week when police searched the home of a teenager accused of stockpiling weapons and bomb-making materials, according to prosecutors. Federal authorities have joined police in investigating the 18 year old suspect, who allegedly was storing the weapons

and materials in Bethesda, Maryland. The Maryland assistant state attorney disclosed the discovery of the map during a court hearing on Tuesday. Police also reportedly discovered range-finding binoculars, a Central Intelligence Agency (CIA) identification, and a Geneva Convention identification, like ones given to contractors in Iraq. Additionally, investigators discovered documents on how to kill from a distance of 200 meters. The CIA and U.S. Defense Department have started their own investigations of the suspect and of an unnamed 17-year-old male, who also has been charged in the case. The Federal Bureau of Investigation and the U.S. Bureau of Alcohol, Tobacco and Firearms are reviewing the case but have not launched their own investigations. The unnamed juvenile, while working as a police intern, allegedly took official stationery to help the suspect obtain chemicals and police equipment, including bullet-resistant vests.
Source: http://www.foxnews.com/story/0,2933,398403,00.html

28. *August 5, La Jolla Light* – (California) **Perpetrator of UCSD bomb hoax sentenced.** A La Jolla, California, resident will serve 15 months in federal custody in connection with a bomb threat he made at University of California, San Diego (UCSD), announced a U.S. attorney. The man, according to court records, admitted that on or about December 5, 2007, he made a series of threatening phone calls and sent one letter to the university warning that bombs had been placed in six campus buildings. The man admitted that the threats were designed to interfere with the activities of UCSD's animal research facilities. After the threats were made, UCSD employees discovered a fake improvised explosive device in a campus research facility where scientists conduct animal testing. The man admitted responsibility for the hoax device.
Source: http://www.lajollalight.com/news/247340-perpetrator-of-ucsd-bomb-hoax-sentenced

[Return to top]

Emergency Services Sector

Nothing to report

[Return to top]

Information Technology

29. *August 6, Associated Press* – (International) **Giant online security hole getting fixed, slowly.** An underlying flaw revealed nearly a month ago in the Domain Name System (DNS), a network of millions of servers that translate words typed into Web browsers into numerical codes that computers can understand, is allowing criminals to silently redirect traffic to Web sites under their control. The problem is being fixed, but its extent remains unknown and many people are still at risk. The gaping security hole enables a scam that targets ordinary people typing in a legitimate Web address. It happens because hackers are now able to manipulate the machines that help computers find Web sites. If done properly, computer users are unlikely to detect whether they have landed at a legitimate site or an evil double maintained by someone bent on fraud. Security experts fear an open season for virus attacks and identity-fraud scams.

Source: http://ap.google.com/article/ALeqM5iGUZJCY0P8h6s6-G-M7ZybPI4VhQD92COS980

30. *August 6, Product-reviews.net* – (International) **Adobe Flash Player download warning: Malware disguised.** There has been coverage from the security community of a nasty worm on many popular social networking sites that is using social engineering lures to get you the user to install a piece of malware, and according to reports the worm posts comments on these such sites that includes links to a fake site. If this link is clicked and followed, users will be told that they need to update their Flash Player. The installer, posted on a malicious site, of course installs malware instead of Flash Player.
Source: http://www.product-reviews.net/2008/08/06/adobe-flash-player-download-warning-malware-disguised/

31. *August 6, PCmag* – (International) **Password stealing trojan on the loose.** Security experts at MicroWorld have reported an alarming increase in the number of infections caused by the ZBot-D Trojan. The ZBot-D Trojan also known as ZBot first surfaced in February 2008 and mostly spreads via emails. It can effortlessly disable the firewall, steal financial data, and can also provide the hacker remote access to the infected system. ZBot has been designed very craftily to perform multiple malicious activities at a given point of time. It can modify system files, create new system processes, and automatically delete cookies in the Internet Explorer URL cache, so that key strokes are recorded and sent to the botnet herder, when unsuspecting users enter their passwords on online banking Web sites. Once any user opens a ZBot infected email, a file named "ntos.exe" is automatically installed in the system folder that adds entries in the registry to automatically invoke the Trojan at the system start up. The Trojan then creates havoc in the system such as, forwarding your personal details to remote websites from where the details are used by hackers and botnet herders, which in turn is sold to criminals for financial gains. It also starts flooding the inbox with loads of Spam and transforms the infected machine into a zombie computer, member of a botnet network. The zombie machines are then used for performing criminal activities.
Source: http://www.pcmag-mideast.com/NewsDetail.aspx?ID=1752

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

32. *August 5, Network World* – (International) **Skype won't say if it decrypts VoIP calls.** Skype, a voice-over-IP (VoIP) phone company, has declined to comment on an online report that alleges that Austrian officials with legal authority to tap VoIP phone communications have no problem listening in on Skype calls, which are encrypted as a

standard part of Skype service. A Skype spokesman would not say whether Skype keeps keys to decrypt calls. It is virtually impossible to figure out for sure from independent research whether Skype keeps encryption keys or not, said the chairman of the Voice Over IP Security Alliance and senior director of security research at TippingPoint. "No one has shown it publicly," he said. "Skype is a closed software package, essentially a black box." The company has on rare occasions allowed outside researchers to examine and verify the security of its encryption, but not whether the keys that can crack the encryption can be retrieved, he said. To allay fears that the calls might not be secure from law enforcement, Skype should open its platform to evaluation by trusted, credible industry experts, he said. In the U.S., the Communications Assistance for Law Enforcement Act (CALEA) forbids requiring that vendors build in back-door decryption, said the vice president for public policy at the Center for Democracy & Technology. "CALEA expressly forbids requiring anyone to be able to decrypt anything," he said. But that does not mean they don't build in key-retrieval anyway. Currently there are no active proposals to force vendors to leave encryption back doors in their VoIP gear.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9111661&taxonomyId=17&intsrc=kc_top

33. *August 5, San Bernardino County Sun* – (California) **Cities explore fiber options.** The city of Grand Terrace is exploring the possibility of hooking into Loma Linda's fiber-optic network as a way to boost economic development. Officials in both cities are in preliminary discussions on a plan to bring a fiber-optic connection to Grand Terrace businesses. Loma Linda has linked 2,000 new homes in the city to high-speed fiber-optic Internet service through its Connected Community Program. Loma Linda University, the Jerry L. Pettis Memorial Veterans Medical Center, and many businesses in town are part of the network. The city is in the process of expanding the four-year-old program to include older homes. Grand Terrace would like to tap into the same technology. Loma Linda's information systems director estimates it would cost somewhere between $1 million and $10 million to bring the network from Loma Linda's westerly city limits to Grand Terrace, which is about four miles away.
Source: http://www.sbsun.com/news/ci_10109656

34. *August 5, CNet*– (National) **Twitter targeted by malware attacks.** Twitter, the popular microblogging service that spread word of California's recent earthquake even as phone lines we jammed, is now being targeted by online criminals. Kaspersky Lab has uncovered a fake Twitter profile created solely for the purpose of infecting people's computers. The profile has posted a link that purports to be a video, but is instead Trojan software masquerading as MP3 files that steal data from the machine, according to the Kaspersky's Viruslist.com blog. The attack is dangerous because it does not require programming skills and could spread easily if it ends up high in Google search engine rankings. That is possible because Google indexes unprotected Twitter profiles.
Source: http://www.download.com/8301-2007_4-10007323-12.html

[Return to top]

Commercial Facilities Sector

35. *August 6, Santa Cruz Sentinel* – (California) **Animal activists could bomb wrong house.** Animal rights activists printed a list in a pamphlet left in a downtown Santa Cruz coffeehouse last week with names and addresses of University of California-Santa Cruz (UCSC) researchers who work with animals in their laboratories. However, several houses were wrongly listed in the pamphlet. This list included a UCSC biologist whose front porch was firebombed early Saturday morning. A Volvo station wagon belonging to another researcher was bombed about the same time. According to a Santa Cruz police spokesman at least three addresses listed on the pamphlet found last week were incorrect. Law enforcement officials declined to specify how many or which addresses were wrong for security reasons. That does not reassure neighbors who fear that animal activists will set fire to the wrong house.
Source: http://www.mercurynews.com/breakingnews/ci_10112636

36. *August 5, Celebrity News Service* – (California) **Bomb threats scare Tom Cruise, Salma Hayek's production companies.** Two Hollywood production companies owned by well known actors have both received bomb threats from an anonymous phone caller, which turned out to be false alarms. United Artists production company, Ventanarosa production company, and talent agency ICM were evacuated when other tenants at the MGM building received a mysterious phone call saying a bomb would be activated at noon. After notifying the Los Angeles Police Department, the building occupants were told to vacate the premises. The property was immediately searched thoroughly for explosives or other suspicious devices. However, nothing suspicious was found.
Source: http://www.allheadlinenews.com/articles/7011846013

[Return to top]

National Monuments & Icons Sector

Nothing to report

[Return to top]

Dams Sector

37. *August 6, Times-Picayune* – (Louisiana) **Levee group slams ASCE investigation.** On Tuesday, a New Orleans nonprofit flood protection watchdog group blasted the American Society of Civil Engineers (ASCE) for failing to complete an investigation of alleged unethical behavior of its staff during the initial investigation of levee failures in New Orleans. The Levees.org founder further criticized delays in the completion of a review of ASCE's peer reviews of natural and man-made disasters, which the industry group commissioned in December after the filing of the ethics complaint. An ASCE spokeswoman said she could not say when the ethics investigation, being conducted by a committee of three former ASCE presidents, will be completed. The Army Corps of Engineers has requested that the ASCE appoint an "external review panel" to advise the Corps-sponsored Interagency Performance Evaluation Task Force (IPET), which was

investigating the causes of flooding during Hurricane Katrina. Since then, the review panel has continued to advise the Corps on changes in policies and construction methods that stemmed from the IPET investigation. It also has published critiques of sections of the IPET's report as they have been completed.
Source: http://www.nola.com/timespic/stories/index.ssf?/base//library-153/1218000700221820.xml&coll=1

38. *August 6, Chico Enterprise Record* – (California) **County sues Water Resources over dam relicensing.** Butte County's years-long battle with the California Department of Water Resources (DWR) over the alleged costs of having the Oroville Dam complex here took a new turn Tuesday when the Board of Supervisors voted to file suit against the state agency. The county maintains that the dam complex costs millions of dollars annually in taxes the county does not receive, and from direct costs related to fire, law enforcement, road improvements, and other issues. DWR, which is currently trying to win a new 50-year license to operate the dam and its power plants from the Federal Energy Regulatory Commission (FERC), has maintained the money that comes to the county and its residents due to tourism more than makes up for any alleged county costs. In the lawsuit, Butte County alleges DWR failed to comply with the California Environmental Quality Act while preparing its environmental impact report, which is required by FERC as part of the relicensing procedures.
Source: http://www.chicoer.com/news/ci_10110049

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.
To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer